Diffie Hellman

Crittografia

Luciano Margara

Unibo

2025

Notazione

Un gruppo è una struttura algebrica formata dall'abbinamento di un insieme non vuoto con un'operazione binaria interna (come ad esempio la somma o il prodotto), che soddisfa gli assiomi di associatività, di esistenza dell'elemento neutro e di esistenza dell'inverso di ogni elemento. Se l'operazione interna è anche commutativa allora il gruppo viene detto Abeliano.
Esempio: $\mathbb{Z}_n$ con l'operazione somma modulo n

Notazione

* è una operazione binaria interna su G (cioè, per ogni a,b appartenente a G, il risultato a*b appartiene a G).

N.B: * indica operazione binaria interna qualsiasi

$(G, *)$ è un gruppo se e solo se

Proprietà associativa:

$\forall a, b, c \in G : \ (a * b) * c = a * (b * c)$

Elemento neutro:

$\exists e \in G, \forall a \in G : \ a * e = e * a = a$

Inverso:

$\forall a \in G, \exists a' \in G : \ a * a' = a' * a = e$

Notazione

$(G, *)$ è un gruppo abeliano se e solo se

$(G, *)$ è un gruppo e vale

Commutatività:

$\forall a, b \in G : \; a * b = b * a$

* è una operazione binaria interna su G (cioè, per ogni a,b appartenente a G, il risultato a*b appartiene a G).

N.B: * indica operazione binaria interna qualsiasi

Notazione

Consideriamo $\mathbb{Z}_n$ con l'operazione somma modulo n
$(\mathbb{Z}_n, +)$ è un gruppo abeliano.
L'elemento 1 è un generatore del gruppo perché qualunque elemento x del gruppo può essere scritto come

$$x = \overbrace{1 + \cdots + 1}^{x \text{ volte}}$$

per questa ragione $(\mathbb{Z}_n, +)$ è un gruppo ciclico

Notazione

Un elemento g si dice generatore di G se ogni elemento di G può essere
ottenuto come una potenza (o un multiplo, se usiamo la notazione additiva) di g.

Sia G un gruppo moltiplicativo. Un generatore $g \in G$ è un elemento di G tale che

$$\{g^i : i \in \mathbb{Z}\} = G$$

Notazione

$\mathbb{Z}_p^*$ gruppo moltiplicativo degli interi modulo p e primi con p (quindi lo zero è escluso)

$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$

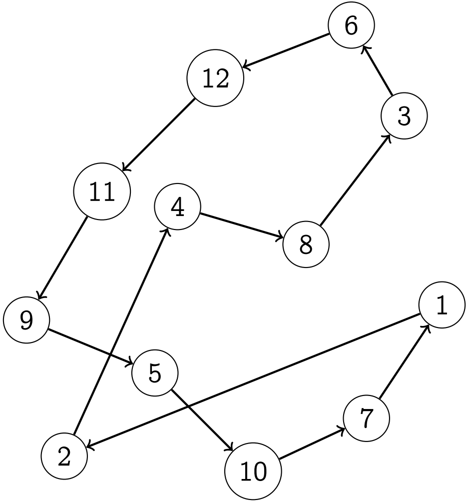
Per ogni valore p primo esiste sempre $g \in \mathbb{Z}_p^*$ tale per cui g è generatore moltiplicativo di $\mathbb{Z}_p^*$

ogni elemento di Zp* può essere scritto come una potenza di g modulo p.

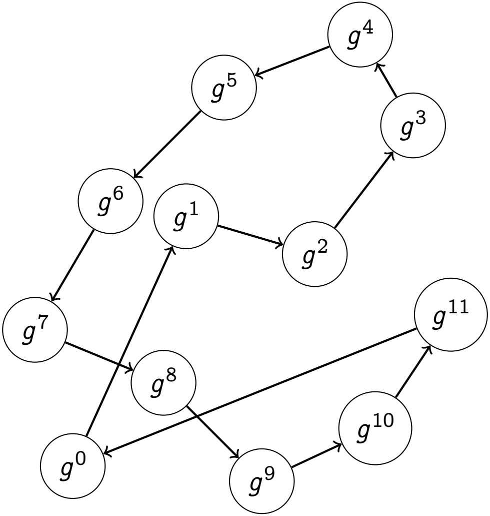
$\mathbb{Z}_{13}^*$

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
2 & 4 & 8 & 3 & 6 & 12 & 11 & 9 & 5 & 10 & 7 & 1 \\
3 & 9 & 1 & 3 & 9 & 1 & 3 & 9 & 1 & 3 & 9 & 1 \\
4 & 3 & 12 & 9 & 10 & 1 & 4 & 3 & 12 & 9 & 10 & 1 \\
5 & 12 & 8 & 1 & 5 & 12 & 8 & 1 & 5 & 12 & 8 & 1 \\
6 & 10 & 8 & 9 & 2 & 12 & 7 & 3 & 5 & 4 & 11 & 1 \\
7 & 10 & 5 & 9 & 11 & 12 & 6 & 3 & 8 & 4 & 2 & 1 \\
8 & 12 & 5 & 1 & 8 & 12 & 5 & 1 & 8 & 12 & 5 & 1 \\
9 & 3 & 1 & 9 & 3 & 1 & 9 & 3 & 1 & 9 & 3 & 1 \\
10 & 9 & 12 & 3 & 4 & 1 & 10 & 9 & 12 & 3 & 4 & 1 \\
11 & 4 & 5 & 3 & 7 & 12 & 2 & 9 & 8 & 10 & 6 & 1 \\
12 & 1 & 12 & 1 & 12 & 1 & 12 & 1 & 12 & 1 & 12 & 1
\end{pmatrix}$$

Generatore di un gruppo finito



Generatore di un gruppo finito



Obiettivo

Alice e Bob vogliono generare una chiave k condivisa.
Alice e Bob non scelgono una chiave, ma la generano cooperando.

Generazione di una chiave segreta condivisa

Alice sceglie a caso un numero primo p, un generatore g di $\mathbb{Z}_p^*$ e un numero intero $a > 0$ che rimane privato.

Alice calcola $A = g^{a} \mod p$

Alice spedisce a Bob (g, p, A)

Bob sceglie a caso un numero b (un numero che rimane privato, anch'esso un intero positivo)

Bob calcola $B = g^{b} \mod p$

Bob spedisce a Alice B

usando il valore A ricevuto da Alice e il suo segreto b.

Bob calcola la chiave segreta $K = A^b \mod p$

Alice calcola la chiave segreta $K = B^a \mod p$

usando il valore B ricevuto da Bob e il suo segreto a.

Calcolo della chiave segreta condivisa (Così, entrambi ottengono la stessa chiave segreta K=g^ab mod p.)

Perché funziona?
La proprietà fondamentale qui è che l'operazione esponenziale è commutativa nel senso degli esponenti: (g^a)^b congruente a (g^b)^a mod p. Quindi, anche se Alice e Bob usano segreti differenti a e b, il prodotto ab è lo stesso indipendentemente dall'ordine, garantendo che entrambi calcolino g^ab mod p.

Esempio

Alice sceglie $p = 7919,\ g = 3\ a = 2500$

Alice calcola $A = 3^{2500} \mod 7919 = 7204$

Alice spedisce a Bob $(3, 7919, 7204)$

Bob sceglie a caso un numero $b = 1222$

Bob calcola $B = 3^{1222} \mod 7919 = 7672$

Bob spedisce a Alice $B = 7672$

Bob calcola la chiave segreta

$$K = 7204^{1222} \mod 7919 = 3989$$

Alice calcola la chiave segreta

$$K = 7672^{2500} \mod 7919 = 3989$$

Semplificando

Alice	Eve	Bob
sceglie p primo		
sceglie g generatore		
	$\rightarrow \underline{(p, g)} \cdots$	$\cdots \rightarrow (p, g)$
sceglie a (privato)		
	$\rightarrow \underline{g^a} \cdots$	$\cdots \rightarrow g^a$
		sceglie b (privato)
$g^b \leftarrow \cdots$	$\cdots \leftarrow \underline{g^b}$	
$k = (g^b)^a$		$k = (g^a)^b$

Sicurezza del protocollo

Alla fine del protocollo entrambi i partner hanno generato la stessa chiave di sessione che viene così utilizzata per le cifrature simmetriche successive. Un crittoanalista passivo può aver intercettato i valori p, g, A, B scambiati in chiaro tra i due partner, ma per calcolare la chiave di sessione deve risolvere l'equazione $A = g^a \ mod \ p$ rispetto ad a, oppure $B = g^b \ mod \ p$ rispetto ad b, ovvero calcolare il logaritmo discreto di A, o di B , che è un problema computazionalmente difficile e quindi improponibile per valori di p molto grandi.

Logaritmo discreto

$$A = g^a$$

$$\log_g(A) = \log_g(g^a) = a$$

Ma noi abbiamo

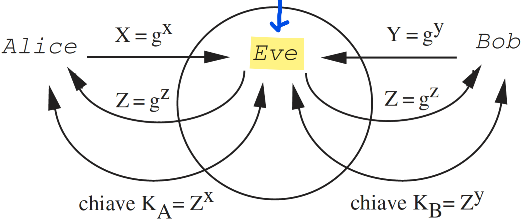
$$A = g^a \; mod \; p$$

e il problema del logaritmo diventa complicato ...

Sicurezza del protocollo

Le insidie non sono però scongiurate perchè un crittoanalista attivo può condurre attacchi distruttivi sul protocollo se è in grado di modificare la comunicazione tra Alice e Bob. Questa situazione, nota come man in-the-middle, permette di compromettere il protocollo DH con grande facilità. Il crittoanalista prende il nome di Eve.

Man-in-the-Middle Attack



Man-in-the-Middle Attack

positivo che mantiene privato

Eve sceglie un intero positivo qualsiasi z che mantiene privato, calcola il valore $Z = g^z \ mod \ p$ e si frappone sul canale bloccando le comunicazioni tra Alice e Bob per sostituirle con le proprie. Eve cattura i messaggi X e Y di Alice e Bob e risponde a entrambi con Z. Alice e Bob interpretano Z come proveniente dall'altro partner e costruiscono le chiavi (diverse) perché non cambia solo l'ordine, ma anche composizione della potenza

$$K_A = Z^x \ mod \ p = g^{xz} \ mod \ p$$

$$K_B = Z^y \ mod \ p = g^{yz} \ mod \ p$$

con cui proseguiranno la comunicazione con Eve che colloquia con Alice usando K_A e con Bob usando K_B